I The Essentials

This first section of six chapters covers several issues that one should be familiar with prior to working with images in an imaging forensics environment. After reviewing the rules and guidelines that govern the use and handling of images in a legal setting, we'll look at how to set up and navigate through Photoshop, Bridge, and Adobe Camera Raw.

Chapter 1 **Best Practices**
Chapter 2 **Reports and Testimony**
Chapter 3 **Basic Imaging Settings**
Chapter 4 **Navigating with Bridge**
Chapter 5 **Camera Raw**
Chapter 6 **Viewing Metadata**

Best Practices

In any aspect of evidence collection, crime scene documentation, and evidence processing, it is important to adhere to best practices in the methods used and the documentation recorded to show that the evidence presented is what it purports to be. Best practices may frequently go beyond the requirements of court so that any legitimate challenge to the procedures or the results can be met. That is, the goal isn't merely to have the evidence admitted into court; the evidence must also hold up to any legitimate challenges once it has been admitted into court.

1

Chapter Contents

Rules of Evidence
Case Law
Four Aspects of Best Practices

Rules of Evidence

The use of digital images in court is determined by rules of evidence and by case law. In both of those areas (at the time of this writing), digital images are allowed as evidence in court (and have been since at least 1991). There are no requirements beyond those required of any photographic image—and that is that they depict what they purport to depict.

The significant portions of the Federal Rules of Evidence are rules 1001 to 1008 (see sidebar). These rules define what is considered an original, what is considered a duplicate, and the burden of proof should there be a challenge. Most states also have their own rules of evidence; many have adopted the wording of the Federal Rules.

Federal Rules of Evidence (Rules 1001—1008)

Rule 1001. Definitions

For purposes of this article the following definitions are applicable:

1. Writings and recordings. "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
2. Photographs. "Photographs" include still photographs, X-ray films, video tapes, and motion pictures.
3. Original. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".
4. Duplicate. A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

Rule 1002. Requirement of Original

To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.

Rule 1003. Admissibility of Duplicates

A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

Federal Rules of Evidence (Rules 1001—1008) *(Continued)*

Rule 1004. Admissibility of Other Evidence of Contents

The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—

1. Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
2. Original not obtainable. No original can be obtained by any available judicial process or procedure; or
3. Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or
4. Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue.

Rule 1005. Public Records

The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with rule 902, or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given.

Rule 1006. Summaries

The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

Rule 1007. Testimony or Written Admission of Party

Contents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by that party's written admission, without accounting for the nonproduction of the original.

Rule 1008. Functions of Court and Jury

When the admissibility of other evidence of contents of writings, recordings, or photographs under these rules depends upon the fulfillment of a condition of fact, the question whether the condition has been fulfilled is ordinarily for the court to determine in accordance with the provisions of rule 104.

Continues

Federal Rules of Evidence (Rules 1001—1008) *(Continued)*

However, when an issue is raised (a) whether the asserted writing ever existed, or (b) whether another writing, recording, or photograph produced at the trial is the original, or (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact to determine as in the case of other issues of fact.

House Committee on the Judiciary, *Federal Rules of Evidence*, 108th Cong., 2nd sess., 2004. Committee Print 8.

Case Law

Case law includes Frye and Daubert challenges, appellate cases, and the plethora of non-challenged cases.

Frye or Daubert hearings may be held as a pretrial hearing to determine the admissibility of scientific evidence in court. The enhancement of fingerprints using digital image processing has been through three Frye hearings (*Commonwealth of Virginia v. Robert Douglas Knight*, 1991; *State of WA v. Eric Hayden*, 1995; *State of Florida v. Victor Reyes*, 2003). In each of these cases, the digital imaging technology met the court requirements and was determined to meet the threshold requirements of Frye. Additionally, the Hayden case was upheld on appeal in 1999. These three cases provide a strong foundation for the use of image processing techniques for image enhancement in court.

Additionally, thousands of cases using digital photographs are used in court every month throughout the United States. It is rare that a digital image is challenged at all, and there have been no cases to date that I am aware of in which a digital photograph has been excluded solely because it is digital.

The rules of evidence and the case law regarding digital images do not prevent legitimate challenges to the veracity of any image or to the legitimacy of any specific adjustment, correction, or enhancement made to an image. For this reason, it is important that anyone involved in presenting images for court use methods that will yield the same results when repeated and use valid imaging forensic techniques.

Four Aspects of Best Practices

The four basic aspects to best practices in imaging forensics are as follows:

- Archive the original image.
- Work only on copies of the original file.
- Use only valid forensic image processing procedures.
- Ensure that all processes are repeatable and verifiable.

Archive the Original Image

An unaltered copy of the original, or primary, image should be archived in its original format. This file should be stored for as long as your agency requires for photographic evidence. Whether this image is stored on a computer hard drive, server, CD, DVD, or other media is not important. What is important is that the image be maintained in its unaltered state and that it is stored in a manner to protect it from damage.

If the original image is a Raw file, the file is by default unalterable. That is, opening a Camera Raw file automatically creates a duplicate of the original, and that opened file must be saved in a different format. It is important to note that some metadata (such as file modification dates) in a Raw file may be changed, but not the image data. Converting Raw files to the open DNG format for archiving could help assure that the files can be opened at any point in the future, even if the camera manufacturer no longer supports the specific original Raw format. The DNG conversion does not alter the Raw file but places it in a larger container, making it a more universal, and less proprietary, format.

If the file is a JPEG or TIFF file, then it is important that policies and/or procedures be in place that require anyone who has access to open only duplicates of these files. This can be easily done by copying the files to a new location—leaving the originals untouched.

The archive should not allow rewriting of files. This will ensure that these original files remain unaltered and will also prevent them from being overwritten by other files that have the same name.

Work Only on Copies

Access to the original images can be easily limited through permissions on a server, passwords on an individual computer, or restricted access to stored media.

If images are stored on a server, access can be restricted through permissions protocols. The ability to write to the server should be restricted only to personnel uploading files. It is highly recommended that this capability be restricted to as few individuals as possible. Permissions can be set to Read and Write to allow uploading and viewing of files. To prevent anyone from making changes to files, deny the Modify permission setting. This is excellent security because it prevents files from being overwritten or changed in any way.

When trained personnel access files (whether from a server, a CD, DVD, or a directory on a personal computer), they can duplicate them to a working directory, leaving the originals untouched. There is never a need to work on the original archived file.

By working only on copies of the archived originals, you can maintain the integrity of the original archived files and can refer to them for comparison with corrected or clarified images.

Valid Forensic Procedures

As a general rule, we can use valid procedures to adjust the quality of the image but not to change the content of the image. But, as with most general rules, there are exceptions. Some techniques are intended to make a qualitative change but result in a change of content. And there are instances when changing the content is necessary.

Overprocessing an image so that image artifacts distort or alter the image content is an example of making changes that result in a change of content. Strong adjustments of contrast or brightness values can result in objects changing size or shape or blending into each other. Caution must be used in making any image adjustments so that qualitative changes are not overapplied.

As to necessary changes of content, examples include adding annotations to an image (as in a court chart) or changing the backgrounds of pictures in a photo lineup so that one individual does not stand out from the rest. In cases where the addition of text, lines, or other data is very obvious, the change stands for itself. In cases where an unusual background in a photo lineup is made to better match the individuals, documentation should be included in a report so that all interested parties are aware of the change.

Many image adjustments can be done in a nondestructive manner with adjustment layers. When you use this feature in Photoshop, the unchanged image resides as the base layer and the image adjustment layer is a separate layer that includes the parameters set by the technician. To make corrections and enhancements to images, one can turn off the adjustment layers and see the unchanged image and then turn on each adjustment layer to display what changes each has made to the image quality. The adjustment layer icon can be accessed to see the parameters used for each adjustment. Masks can be included for each adjustment layer to apply the adjustment to specific portions of the image.

Valid forensic methods are repeatable with similar results, are applied to groups of pixels, and provide explainable and predictable results. Image adjustments should be applied to a copy of the original, and an audit trail (either the procedure itself or notes) should be a part of any valid forensic workflow.

Repeatable Processes

It is frequently necessary to make adjustments to an image. Perhaps the image has a green cast from fluorescent lights or has very little contrast from being photographed on an overcast day. Or, perhaps a fingerprint image is obliterated by a stain and needs enhancement to see fine details. In all of these instances, changes need to be made to the image to improve its quality.

With any of these changes, the technician who made them must work on a copy of the original, use valid imaging forensic techniques, and be able to repeat them if required to do so. To enable the repeatability of the process, an audit trail may be used. An audit trail is the recording of the steps used to make any adjustments so that they can be repeated to obtain similar results. The audit trail may be a standard procedure that is routine and consistent, handwritten notes, a text document containing notes, or data that contains this information stored within the file itself, such as Photoshop's History Log.

Some adjustments are basic—such as a brightness or contrast adjustment—and may always be performed using the same techniques with similar settings. In these instances, retaining a copy of the modified image and an audit trail of the changes may not be necessary. The key here is that the procedure is a common one, is a standard routine, is a valid procedure, and can be easily repeated with similar results—even without notes. In such an instance, the standard operating procedure becomes the audit trail.

Audit Trail and History Log

When procedures are used that go beyond basic adjustments, a copy of the modified image should be retained. And there should be an audit trail of all steps used to make the adjustments. As mentioned in the preceding section, an audit trail may be handwritten notes, a text file, or data contained within the image file itself. With Photoshop CS and above, this can be done automatically using the History Log feature. It is important to note that Photoshop's History Log is not active by default, and must be turned on in the General Preferences window (Figure 1.1).

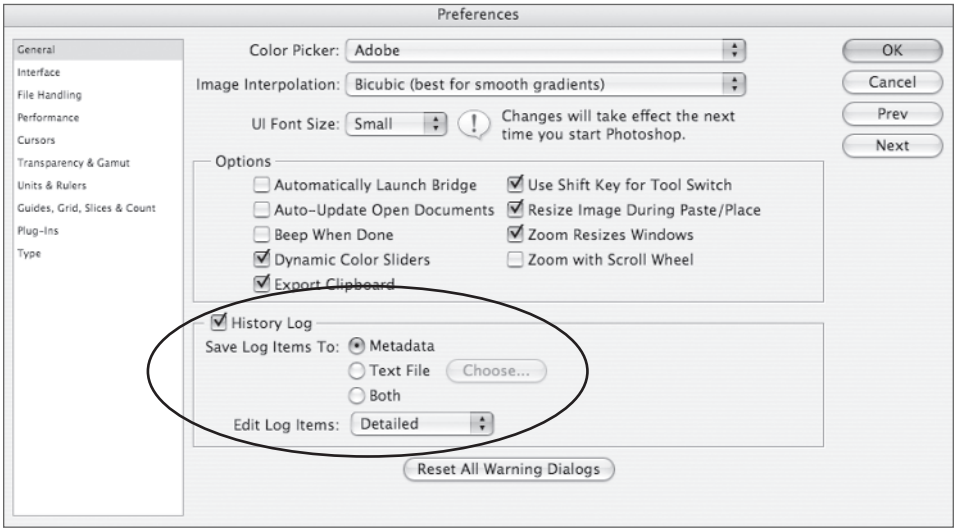

Figure 1.1 The History Log must be activated in the General Preferences window.

The History Log can be viewed in Adobe Bridge (see Chapters 4 and 6) or by choosing File > File Info in Photoshop and then clicking the History Log tab (Figure 1.2). See Chapters 3 and 6 for more information about the History Log.

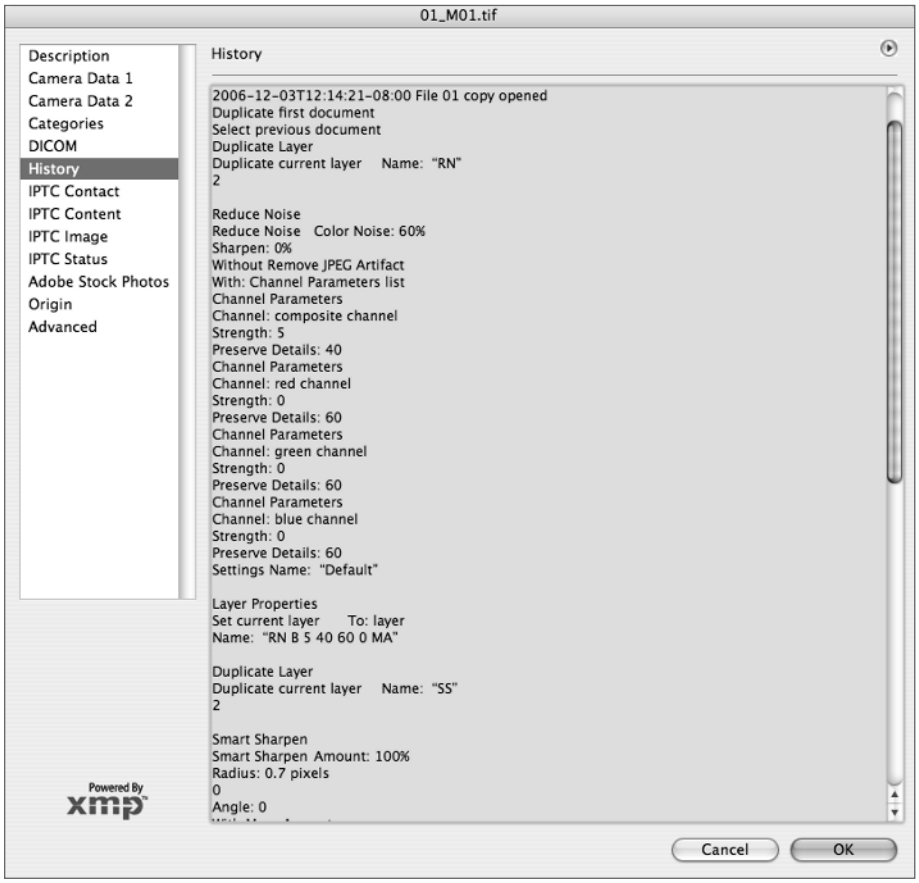

Figure 1.2 The History Log is available as one of the tabs in the File Info window.

Summary

Utilizing best practices goes beyond the requirements of court, case law, and rules of evidence. Best practices provide us with standard operating procedures in your workflow to maintain the integrity of your images and procedures. By maintaining a digital negative, only working on copies of the original, using only valid forensic procedures, and maintaining an audit trail for any nonstandard enhancements or analysis, you can be assured that you have done the due diligence needed in forensics.